AMENDMENT TO THE CLAIMS

1. (Original) A computer-implemented method for enhancing the security of informational interactions with a biometric device, comprising:

pre-establishing an encryption relationship between a computing device and the biometric device;

generating a session packet, encrypting it, and transmitting it to the biometric device; and

receiving a biometric information packet, decrypting it, and making a determination, based on a content of a collection of information contained in the decrypted biometric information packet, as to whether or not to utilize a collection of biometric data contained in the decrypted biometric information packet.

2. (Original) The method of claim 1, wherein generating a session packet comprises generating a session number and storing it in the session packet.

3. (Currently Amended) The method of claim 2, further comprising storing the session number in a database associated with the ~~computingdevice~~ computing device.

4. (Original) The method of claim 1, wherein generating a session packet comprises obtaining a session key and storing it in the session packet.

5. (Original) The method of claim 4, further comprising storing the session key in a database associated with the computer.

6. (Original) The method of claim 4, wherein receiving a biometric information packet and decrypting it comprises receiving a biometric information packet and decrypting it with an encryption key that is complimentarily related to the session key.

7. (Original) The method of claim 4, wherein obtaining a session key comprises generating a public key portion of a PKI key pair.

8. (Original) The method of claim 7, wherein receiving a biometric information packet and decrypting it comprises receiving a biometric information packet and decrypting it with a private key portion of the PKI key pair.

9. (Original) The method of claim 1, wherein receiving a biometric information packet and decrypting it comprises receiving a biometric information packet and decrypting it with an encryption component that is independent of the pre-established encryption relationship.

10. (Original) The method of claim 1, wherein generating a session packet comprises generating a session time stamp and storing it in the session packet.

11. (Original) The method of claim 1, wherein generating a session packet comprises:

generating a session number and storing it in the session packet; and

obtaining a session key and storing it in the session packet.

12. (Original) The method of claim 11, further comprising storing the session number, the session key and a session time stamp in a database associated with the computer.

13. (Original) The method of claim 1, wherein making a determination comprises comparing a session number to a list of valid values.

14. (Original) The method of claim 1, wherein making a determination comprises evaluating a session time stamp to determine whether the biometric information packet was received within a predetermined time period.

15. (Original) The method of claim 1, wherein making a determination comprises comparing a data representation of a user's biometric information to at least one data representation of biometric information stored in a database.

16. (Original) The method of claim 1, wherein making a determination comprises:

comparing a session number to a list of valid values;

evaluating a session time stamp to determine whether the biometric information packet was received within a predetermined time period; and

comparing a database representation of a user's biometric information to at least one data representation of biometric information stored in a database.

17. (Original) The method of claim 1, wherein pre-establishing an encryption relationship comprises storing a first encryption component with the computing device and a second encryption component with the biometric device, one of the first and second encryption components being configured to decrypt information that has previously been encrypted utilizing the other of the first and second encryption components.

18. (Original) The method of claim 17, wherein encrypting the session packet comprises encrypting the session packet utilizing one of the first and second encryption components.

19. (Original) The method of claim 1, wherein pre-establishing an encryption relationship comprises storing a first part of a PKI key pair with the computing device and a second part of the PKI key pair with the biometric device.

20. (Original) The method of claim 19, wherein encrypting the session packet comprises encrypting the session packet utilizing one of the first and second parts of the PKI key pair.

21. (Original) The method of claim 1, wherein pre-establishing an encryption relationship comprises storing a first part of a static encryption key pair with the computing and a second part of the static encryption key pair with the biometric device, one of the first and second parts being

configured to decrypt information that has previously been encrypted utilizing the other part.

22. (Original) The method of claim 21, wherein encrypting the session packet comprises encrypting the session packet utilizing one of the first and second parts of the static encryption key pair.

23. (Original) A data packet for transmission from a computer to a biometric device during a process of authentication within a biometric security system, the data packet comprising:

a session key, the session key being an encryption key configured to be utilized to encrypt data.

24. (Original) The data packet of claim 23, wherein the session key is a public key portion of a PKI key pair.

25. (Original) The data packet of claim 23, further comprising a session number.

26. (Original) The data packet of claim 25, wherein the session number is a value that corresponds to a session initiated when the data packet is generated.

27. (Original) A biometric device configured to support a secure transfer of biometric information to a computing device, the biometric device comprising:

a biometric information receiver configured to capture an individual's biometric information;

a processor configured to process the biometric information and produce a digitized representation thereof;

a memory accessibly connected to the processor; and

an encryption component stored in the memory, the processor being configured to receive an encrypted session packet from the computing device and decrypt it utilizing the encryption component.

28. (Original) The biometric device of claim 27, wherein the encryption component is implemented as firmware.

29. (Original) The biometric device of claim 27, wherein the encryption component is implemented in association with a flash memory application.

30. (Original) The biometric device of claim 27, wherein the encryption component is one part of a PKI key pair.

31. (Original) The biometric device of claim 27, wherein the encryption component is one part of a static encryption key pair.

32. (Original) The biometric device of claim 27, wherein the processor is further configured to place the digitized representation into a biometric information packet.

33. (Original) The biometric device of claim 32, wherein the processor is further configured to encrypt the biometric information packet utilizing a specialized encryption component contained in the session packet.

34. (Original) The biometric device of claim of 33, wherein the processor is further configured to transfer the encrypted biometric information packet to the computer.

35. (Original) A computer readable medium having instructions stored thereon which, when executed by a computing device, cause the computing device to perform a series of steps comprising:

receiving a session initiation command;

generating a session packet;

encrypting the session packet;

transmitting the encrypted session packet to a biometric device;

receiving a biometric information packet from the biometric device;

decrypting the biometric information packet; and

determining, based on a content of a collection of authentication information contained in the decrypted biometric information packet, whether or not to utilize a collection of biometric data contained in the decrypted biometric information packet.

36. (Original) The computer readable medium of claim 35, wherein generating a session packet comprises generating a session number and storing it in the session packet.

37. (Original) The computer readable medium of claim 36, further comprising the step of storing the session number in a database associated with the computing device.

38. (Original) The computer readable medium of claim 35, wherein generating a session packet comprises obtaining a session key and storing it in the session packet.

39. (Original) The computer readable medium of claim 38, further comprising the step of storing the session key in a database associated with the computer.

40. (Original) The computer readable medium of claim 38, wherein receiving a biometric information packet and decrypting it comprises receiving a biometric information packet and decrypting it with an encryption key that is complimentarily related to the session key.

41. (Original) The computer readable medium of claim 38, wherein obtaining a session key comprises generating a public key portion of a PKI key pair.

42. (Original) The computer readable medium of claim 41, wherein receiving a biometric information packet and decrypting it comprises receiving a biometric information packet and decrypting it with a private key portion of the PKI key pair.

43. (Original) The computer readable medium of claim 35, wherein generating a session packet comprises generating a session time stamp and storing it in the session packet.

44. (Original) The computer readable medium of claim 35, wherein determining comprises comparing a session number to a list of valid values.

45. (Original) The computer readable medium of claim 35, wherein determining comprises evaluating a session time stamp to determine whether the biometric information packet was received within a predetermined time period.

46. (Original) The computer readable medium of claim 35, wherein encrypting the session packet comprises encryption the session packet with a first encryption component that is complimentarily related to a second encryption component maintained on the biometric device, one of the first and second encryption components being configured to decrypt information that has previously been encrypted utilizing the other of the first and second encryption components.

47. (Original) The computer readable medium of claim 46, wherein the first and second encryption components are a PKI key pair.

48. (Original) The computer readable medium of claim 46, wherein the first and second encryption components are a static encryption key pair.